9

FOR IMMEDIATE RELEASE

OpenConnect Systems Announces the Industry's First Secure Encrypted Java

DALLAS--June 10, 1996--OpenConnect Systems, Inc. has announced the availability of a new secure version (1.2.2 Beta) of its award-winning OC://WebConnect tm Web 3270 Server for Java tm . A first in the industry, this evaluation version of OC://WebConnect makes encryption-secure Java data stream exchanges between a Java-capable web browser on the desktop and an enterprise web server, via the public Internet or private Intranets a reality. This breakthrough means that corporate legacy data can now be securely accessed by properly authorized users no matter where they are in the world, using a Java-capable web browser.

In making the announcement, OpenConnect President and CEO Stephen J. Clark said, "We've implemented the widely accepted, robust offerings of RSA Data Security, a well-respected industry standard for secure data transfer, into our latest release. Java, of course, has numerous built-in security functions, and that capability combined with proven RSA technology makes this a perfect solution for extending the availability of mission-critical enterprise information. This new version of OC://WebConnect implements Diffie-Hellman Public Key Exchange for convenient, secure, encryption-key management and uses industry standard data encryption algorithms, allowing the highest commercially available security safeguards. This removes the barrier for wider deployment of Internet technologies within enterprise Intranets or over the public Internet."

Establishing the necessary key management infrastructure is a major and costly task in deploying secure encrypted solutions. OC://WebConnect enables rapid deployment of its encrypted solution to thousands of users without this infrastructure and associated costs.

OC://WebConnect establishes the private, symmetric encryption key necessary at both the web server and Java applet using the patented Diffie-Hellman Public Key Exchange for each connection. The encryption key is valid for only one connection and then discarded. A new key is derived for each subsequent session. With the OpenConnect solution no encryption keys are entered by the user; no disks containing key information are inserted, and no third-party security server must be installed and maintained. As a standard feature of OC://WebConnect, users save in the cost of acquisition and in the cost of ownership, and the implementation provided within OC://WebConnect ensures that companies can provide the highest levels of security immediately.

RSA Data Security, Inc. President, Jim Bidzos said, "We are extremely pleased for our technology to be an integral part of OpenConnect's leading-edge products. This bold implementation takes maximum advantage of RSA Data Security, Inc. offerings and is an industry first for integration with Java. The issue of secure access to enterprise information is foremost in the minds of most organizations' managers, and OC://WebConnect's innovative architecture, coupled with RSA's underlying authentication and encryption technology makes it possible."

RSA Data Security, Inc. is considered the industry standard for providing secure mechanisms for transmitting sensitive data over the Internet. Through a technology licensing agreement, OpenConnect has extended RSA's encryption technology to Java applets, allowing automatic and transparent exchange functions to encrypt data flows between end users and the OC://WebConnect server. As with the initial version of OC://WebConnect, users need only have a Java-capable browser in order to access host system information. OpenConnect's Development Manager for Internet Products, Adam Allard stated, "This implementation is based on our porting of RSA's B-Safe Library into Java. By porting RSA encryption code into Java classes, numerous security applications in Java are possible, including a wide range of cross-platform functionality."

Bruce Robertson, program director for the META Group's Global Networking Strategies Service, said, "The requirement for secure data communication rises rapidly with the size and strategic importance of legacy system information that must be shared. Organizations are understandably reluctant to use the power of the Internet until they know it is safe, and the new implementation of OC://WebConnect looks like a viable response to the Internet information security problem." The lack of Internet security for data transmission has long been a concern of enterprise managers. Current OC://WebConnect users believe this new release provides what is needed to protect corporate assets. Miles Rice, application program analyst for Penn State University's Financial Information Systems, said, "This secure Java approach will certainly help me sleep better at night. We work with very sensitive financial data and can't afford slip ups that might occur in an unsecured environment." First Union National Bank's Columbus Cooper, said, "With this enhancement, we will certainly be able to provide our customers even wider access to our banking services."

OC://WebConnect's newest evaluation release includes all the functionality of the first OC://WebConnect release, now generally available as OC://WebConnect Gold (V2.1), this includes 3270, 5250 and user-configurable keyboard mapping. Additionally, the evaluation version now contains RSA security, VT220 subset emulation, support for RUI connection to Microsoft SNA Server and numerous administration tools for "browser-powered" server administration and configuration.

OC://WebConnect was selected as the NetWorld+Interop '96 Best of Show product in the Internet category. IDC Analyst Elisabeth Rainge believes the market is ready for this type of product. Rainge said, "The 3270-WWW gateway meets the requirements of new market opportunities, such as the use of Intranets and the Internet for interbusiness communications." The OC://WebConnect server software converts standard host data flows into Java data flows (and vice versa), permitting multi-session, "persistent" connection access to existing business application. The latest OC://WebConnect evaluation release is available for immediate download by connecting to OpenConnect's home page at http://www.oc.com.

More than 1,000 organizations worldwide have accessed and evaluated OC://WebConnect via the World Wide Web since its initial availability more than a month ago. The general availability Gold release V2.1, can be licensed now and pricing includes future release enhancements and upgrades, such as the security encryption features currently in the evaluation version. Pricing ranges from $49 to $319 per session, based on the number of concurrent users.

Dallas, Texas-based OpenConnect Systems, Incorporated supplies companies worldwide with innovative information technology solutions. With more than 2,500 systems installed in 60 countries, including 40 of the U.S. Fortune 50 companies, OpenConnect Systems is a leading provider of connectivity, interoperability and internetworking products and services.

--30--

CONTACT:
OpenConnect Systems, Inc.
George W. Macintyre,
214/484-5200

gmac@oc.com
or
MarkeTech Associates
Brian L. Moran,
214/960-0551
mtabrian@aol.com.

| **Press Releases** |
What's New?	**What's Old?**	**Download FREE Publications & Software**
RSA & Partner Products	**RSA Labs**
FAQ on Cryptography	**FTP Server**	**About ...**
Contact Sales	**Contact Technical Support**

Contact RSA Data Security, Inc.:

100 Marine Parkway, Suite 500
Redwood City, CA 94065-1031
phone: 415-595-8782
fax: 415-595-1873
Website: http://www.rsa.com/

Website feedback or comments can be sent to : WEBMAVEN@RSA.COM

Last Updated: Tuesday, June 11, 1996

The cryptography "gold standard" of professional developers worldwide

BSAFE™ 3.0 RSA's comprehensive cryptography engine for software developers

Introducing BSAFE 3.0

BSAFE 3.0 is the newest release of the world's most popular cryptography toolkit. Fully compatible with keys and data from previous versions, BSAFE 3.0 is a portable C programmer's toolkit that allows developers to integrate state-of-the-art privacy and authentication features into virtually any application. BSAFE 3.0 provides the programmer with a complete palette of the most popular and trusted cryptographic algorithms, including Triple-DES, RC5, and of course the patented RSA Public Key Cryptosystem,™ the worldwide standard for Internet security. New in BSAFE 3.0 is support for the DSA and SHA1 U.S. government signature and hashing algorithms.

Easy, Full-Featured Development Environment

BSAFE 3.0 can dramatically reduce the cost associated with development of secure applications by giving developers a big head start. With BSAFE, any programmer can develop secure applications — without a background in cryptography, mathematics or number theory. Best of all, by using the toolkit from the most trusted and experienced company in the cryptography business, you won't be troubled by embarrassing and costly software recalls that often result from failed "homegrown" security techniques. BSAFE features an object-oriented API utilizing data abstraction, providing for more efficient development. BSAFE 3.0 is also re-entrant, so it can be shared by many applications at once — a necessity in today's advanced multitasking operating environments. Long, computationally-intensive cryptographic operations are interruptible or even cancelable, and there are a variety of platform-specific optimizations available.

GENUINE
RSA™
ENCRYPTION ENGINE

Algorithms: Flexibility and Performance

BSAFE 3.0 includes routines for the patented RSA and Diffie-Hellman public-key techniques; the DSA government signature algorithm; the popular DES. Triple-DES and DESX secret-key ciphers; the exportable RC2 and RC4 variable key size ciphers; the high-performance RC5 symmetric block cipher; Bloom-Shamir secret sharing and key escrow; the MD2, MD5 and SHA1 hashing algorithms; and improved routines for pseudorandom number generation. And you'll be able to use these algorithms at unprecedented levels of performance — algorithms that function up to 5 times faster than previous versions of BSAFE. That means with BSAFE you'll be able to implement high-bandwidth crypto applications, like secure video, totally in software — without resorting to expensive special-purpose crypto hardware.

What about Standards?

BSAFE is the world's best-selling crypto toolkit, so naturally it can support virtually any global security standard — in fact, many standards were written around the BSAFE toolkit! That means you can talk securely to just about anybody, whether they're speaking SSL, S/HTTP, SEPP, STT, S/MIME, S/WAN, IPSec or PCT. And of course, BSAFE fully supports PKCS, (the Public Key Cryptography Standards) the internationally-recognized public-key interoperability specifications.

Ready for the Future

BSAFE 3.0 was designed to be modular, so you can link in only the algorithms you need. It's also extensible, so you can insert new algorithms in the future — no matter where technology or government specifications take you. BSAFE also supports multiple key and data representations including previous BSAFE 1.x formats, BSAFE 2.x formats and ASN.1 BER (Basic Encoding Rules). Consequently, development is faster and applications built with BSAFE 3.0 enjoy better "forward compatibility" with future encryption techniques and standards.

Unbeatable References

Some of the world's most talented development teams chose RSA's BSAFE toolkit to provide the cryptography built into all of these best-selling applications:

Novell Netware™
secure network operating system

Netscape Navigator™ Browsers & Electronic Commerce Servers
secure Internet browsers and servers

Lotus Notes™
secure workgroup software

Digital Internet Tunnel™
secure VPN via the Internet

Oracle SQL*Net™
secure client/server database

Microsoft Windows 95™
operating system security

...and many, many more. Your application can be on this list, too. With BSAFE, your developers can bring the security benefits of professional cryptography into any application you wish to build — quickly, easily and inexpensively.

BSAFE 3.0 Specifications

Features

- General purpose, low-level cryptography engine
- Backwards-compatible with BSAFE 1.x and BSAFE 2.x keys and data
- Supports the Public Key Cryptography Standards (PKCS)
- Suitable for real-time encryption/ authentication applications
- Supports the following cryptographic techniques:
  - RSA Public Key Cryptosystem
  - RSA Digital Signatures
  - Diffie-Hellman Key Agreement
  - Digital Signature Algorithm (DSA/DSS)
  - Data Encryption Standard (DES)
  - Triple-DES
  - Extended Data Encryption Standard (DESX)
  - RC2 Variable-Key Size Symmetric Block Cipher
  - RC4 Variable-Key Size Symmetric Stream Cipher
  - RC5 Variable-Key Size Symmetric Stream Cipher
  - MD Hashing Algorithm
  - MD2 Hashing Algorithm
  - MD5 Hashing Algorithm
  - SHA1 Hashing Algorithm
- Supports user-definable key sizes up to 2048 bits
- Modular and extensible algorithm framework can easily accommodate new algorithms and standards as needed
- Object-oriented, portable C API
- Re-entrant, interruptible and cancelable cryptographic operations
- Hardware-specific algorithm optimizations available
- Support for multiple key and data representations including ASN.1 BER

Potential BSAFE 3.0 Applications

- Secure Internet Browsers and Servers
- Encrypted Electronic Mail
- Secure Electronic Commerce
- Client/Server Security
- Encryption of Local & Archived Files
- Network User and Service Authentication
- Kerberos Enhancement and Extension
- Secure Software Distribution (CD-ROM)
- Broadcast Encryption
- Voice and Video Encryption
- Digitally Signed Electronic Forms & Workflow
- Encrypted Database and other Client/Server Applications
- Intellectual Property Protection
- Virus Detection
- Secure Remote Access and TCP/IP

System Requirements

Platforms:	DOS, Windows, Windows 95, Windows NT, OS/2, Macintosh, AT&T SVR4 UNIX (Intel), HP/UX, SunOS, Solaris, IBM AIX, NeXT, Silicon Graphics, SCO UNIX, Alpha VMS, VAX VMS, ports to other platforms available.
Memory:	5-20K per algorithm used, application dependent

Related RSA Product Offerings

End-users requiring an application that provides integrated encryption and emergency access capabilities for file and document security should examine RSA Secure, RSA's award-winning file system security extension.

Developers needing to integrate security into store-and-forward based messaging applications like e-mail, e-forms, EDI or electronic commerce should consider TIPEM, RSA's standards-based Toolkit for Interoperable Privacy-Enhanced Messaging.

Developer & Runtime Pricing

See the latest RSA Price Sheet for individual, 5-user and 10-user developer object-code pricing, and quantity runtime distribution pricing.

RSA Licensing

BSAFE 3.0 object or source code can be inexpensively licensed from RSA for inclusion in an application that you intend to market. Royalties and license terms depend on your application type. Contact your RSA representative for a copy of our standard license agreement and a quote.

Contacting RSA

RSA DATA SECURITY, INC.

RSA Data Security, Inc.
100 Marine Pkwy Ste. 500
Redwood City, CA 94065
Phone: 415-595-8782
Facsimile: 415-595-1873
info@rsa.com
http://www.rsa.com/

RSA products contain proprietary, confidential, and/or trade secret RSA encryption algorithms and subroutines. Applications developed with RSA products, if distributed or sold, are subject to additional licensing. Source code licensing is also available. Contact RSA for details.

10

W&V
Weber & Volzing, Inc.
Certified Shorthand Reporters

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ROGER SCHLAFLY,)
)
Plaintiff,)
)
vs.) No. CV 94 20512 SW (PVT)
)
PUBLIC KEY PARTNERS)
and RSA DATA)
SECURITY, INC.,)
)
Defendants.)
)

CERTIFIED COPY

DEPOSITION OF WHITFIELD DIFFIE

Date: Monday, October 23, 1995

Time: 10:00 a.m.

Location: Law Offices of Thomas R. Hogan
60 South Market Street, Suite 1125
San Jose, California 95113

A I was in very regular communication with Hellman. Merkle was at that time at -- at Berkeley and I talked to him intermittently.

MR. SCHLAFLY: Okay. I'll give you another document, Exhibit CH.

(Whereupon, Plaintiff's Exhibit CH was marked for identification.)

Q BY MR. SCHLAFLY: Do you recognize that document?

A Yes.

Q Did you write the document?

A I wrote it jointly with Marty Hellman, yes.

Q And what is that document?

A It's a paper called "Multiuser Cryptographic Techniques" that was given at the National Computer Conference in 1976.

Q Do you know what month that conference was in?

A It was -- began the 7th of June and I think it ran three days.

Q And you presented this paper at that conference?

MR. FLINN: Objection. Asked and answered. You can read it back. It's there.

MR. SCHLAFLY: I think he said the paper was presented, but I don't think that he said he presented it.

THE WITNESS: I presented it.

A Yes.

Q -- or afterwards?

A Yes, previous to the conference.

Q Did copies go to other people?

A I assume so.

Q And who would have handled that?

A Marty.

Q And Marty refers to Martin Hellman?

A Martin Hellman.

Q Who was a Stanford professor at that time?

A I assume he was either assistant or associate professor at that time. I don't --

Q But he was on the Stanford faculty?

A That's correct.

Q Do you know who actually typed this paper, Exhibit CH?

A I typed Exhibit CH. The conference typeset the final result.

Q And any copies of Exhibit CH that might have been distributed would have been by Hellman or Stanford; is that correct?

MR. FLINN: Objection. Calls for speculation, lacks foundation.

Q BY MR. SCHLAFLY: Did you personally distribute copies of Exhibit CH?

A I don't remember distributing any. That's false. I must amplify. I personally gave one to a guy named Blatman, Peter Blatman. B-L-A-T-M-A-N, I believe. I think it has only one T.

Q Who is Mr. Blatman?

A He was a graduate student at the University of California at Berkeley. He is the person through whom I met Ralph Merkle. And he was introduced to me by Lance Hoffman. He was a faculty member at Berkeley.

Q Did you mail a copy to him?

A I probably handed it to him in person.

Q Where did you see him?

A I saw him frequently at that time. I don't remember the occasion of giving him the copy, but it could have been at dinner or it could have been in conjunction to driving back and forth to Stanford. He attended a seminar that Marty and I ran on cryptography.

Q His driving back and forth to Stanford?

A I drove him. I had a car.

Q Oh. Where were you living at the time?

A Berkeley.

Q Oh. You lived in Berkeley and worked at Stanford at that time?

A That's right.

MR. SCHLAFLY: I see. Okay. I'd like to

MR. SCHLAFLY: Let's go back on the record.

MR. FLINN: My copy of Exhibit CA that was furnished to me as part of the plaintiff's summary judgment papers does not contain the title page and abstract that is in the copy being shown to the witness. And I don't know whether other people's copies have that or not, but the record should reflect that the actual exhibit does have the cover page.

MR. SCHLAFLY: Okay. I don't understand that. Mr. Moore, does your copy of Exhibit CA have the title page and abstract?

MR. MOORE: We are getting used to asking questions. Yes, my copy does appear to have the cover page.

MR. FLINN: I hope the court's copy had a cover page, that's all.

MR. SCHLAFLY: I hope so. But thanks for pointing that out. I better check on that.

Q BY MR. SCHLAFLY: Okay. Mr. Diffie, did you write this document?

A Yes.

Q First of all, do you recognize this document?

A I recognize it. I wrote it jointly with Marty Hellman.

Q And what is it?

A It's a paper called "New Directions in Cryptography" that appeared in November, 1976 in the IEEE Transactions on Information Theory.

Q Is this the paper that was submitted on or about June 3rd, 1976, as referenced in Exhibit U?

A Yes, it is.

Q And what date is on this paper?

A August, 1976.

Q Did you distribute copies of this paper to anyone?

A I don't recall doing so.

Q Do you know if anyone distributed copies of this paper?

A No, I don't know.

Q Can you explain why it is dated August, 1976, if it was submitted in June, 1976?

A I assume this version represents the corrections, the result of correcting the galleys. I think it was edited to incorporate any changes made by the editors of the journal.

Q Were there other versions?

A I assume there was a version of June 3rd, 1976 or whatever that date was that was sent to the journal. This one bears the designation it will appear and therefore was produced later, after --

apparently after the commitment to publication was made by the journal.

Q Did you circulate any version of this paper before publication in the journal?

A I do not remember doing so.

Q Do you know of any versions being circulated?

A No. I do not know of any versions being circulated.

Q Does that come as a surprise to you that I am showing you this copy?

A No.

Q Why?

MR. FLINN: That's an entirely improper question. The witness' emotional reaction or lack thereof to what documents you put in front of him is none of your business.

Q BY MR. SCHLAFLY: Okay. Let me rephrase it. Did you attempt to keep the paper a secret?

A I'm sure we didn't.

Q If I had called you up in August of 1976 and asked you for a copy, would you have given me a copy?

MR. FLINN: Objection. Calls for speculation. You don't have to answer that question.

THE WITNESS: My answer is I don't know.

Q BY MR. SCHLAFLY: Did anybody do that?

A I don't remember anyone doing it.

Q Do you know of any explanation for how I might have gotten a copy of this paper?

MR. FLINN: Objection. Calls for speculation.

MR. SCHLAFLY: I'm not asking him to speculate. I'm asking if he knows of a way in which I might have gotten a copy of this paper.

MR. FLINN: I'm sorry. That calls for speculation. You don't have to answer the question.

THE WITNESS: Roger, I don't know how you got this paper.

Q BY MR. SCHLAFLY: Okay. Let's go back to your talk at the National Computer Conference. Was that talk open to the public?

MR. FLINN: Objection. Asked and answered.

THE WITNESS: I'm not sure he's asked exactly that question. The talk was I presume open to conference attendees.

Q BY MR. SCHLAFLY: Could any member of the public have attended the conference?

A I am not aware of any restriction on attending the conference other than paying I assume some fee.

Q Okay. At your talk, did you hand out any copies of any papers?

A I did not.

Q Did you --

A At least, I do not recall handing out any.

Q Okay. Did you show any slides or use an overhead projector?

A I showed thirty-five millimeter slides.

Q Do you have copies of the slides here?

A Yes.

Q Which one is it?

A No, it's the other one (indicating).

Q This (indicating) is it?

A Uh-huh. Those are xerox copies of the handwritten pages from which the thirty-five millimeter slides were photographed. Why there's no title slide, I don't know.

MR. MOORE: For the record, the witness appears to be referring to documents that are Bates stamped DIF 025 through DIF 044.

MR. FLINN: Do I have a Bates stamped set?

MR. MOORE: Not as yet, it appears.

MR. SCHLAFLY: Can we enter this into the record as Exhibit D-1?

(Whereupon, Plaintiff's Exhibit D-1 was marked for identification.)

(Whereupon, there was a discussion off

the record.)

Q BY MR. SCHLAFLY: Are we back on the record? Okay. Mr. Diffie, were any copies of these slides distributed?

A I don't remember distributing any.

Q As far as you know, these are the only copies?

A As far as I knew, those were the only copies.

Q Okay. I'm looking at a slide titled "Matrix Example" about halfway through.

MR. FLINN: What's the number on the page?

THE WITNESS: Oh, how neat.

MR. SCHLAFLY: I'm sorry. Mine aren't numbered.

THE WITNESS: 034.

MR. SCHLAFLY: May I use yours?

MR. MOORE: You may.

Q BY MR. SCHLAFLY: Okay. What does that mean?

MR. FLINN: Objection. Calls for expert opinion.

MR. SCHLAFLY: I'm not asking an opinion, I'm just asking what it is.

MR. FLINN: It's not something a lay person could answer, so only an expert could answer what it is. If you ask him what recollection he has

MR. FLINN: Objection. Calls for speculation, calls for expert opinion. He testified he doesn't remember the document, so for him to read that and analyze it and bring to bear some fresh judgment as to the relationship to some other concept or theory --

MR. SCHLAFLY: All right. We'll ask Mr. Hellman about it. The next document is entitled "New Directions in Cryptography, Talk Given at IBM Watson Lab." Can somebody give me a copy with Bates numbers on them?

MR. MOORE: Yes, Roger.

MR. SCHLAFLY: You're such a swell guy. All right. This will be -- please label this Exhibit D-5.

MR. MOORE: Off the record for a moment, Roger.

(Whereupon, there was a discussion off the record.)

(Whereupon, Plaintiff's Exhibit D-5 was marked for identification.

Q BY MR. SCHLAFLY: Okay. Document D-5 has Bates number DIF 045 through DIF 075. Do you recognize this?

A Yes, I recognize this document.

Q What is it?

A It is the foils for a lecture I gave at IBM Watson Labs in Yorktown Heights. And it's dated 6 July 1976, so I assume that's the date of the lecture. That's not something I'd remember.

Q Who was this a lecture to?

A I do not remember whether it was in any regularly scheduled series. It was a lecture to a small number of people, between one and two dozen, I would speculate, who probably mostly came from the mathematics department, but I don't know whether it was -- how it was advertised within the lab.

Q The math department of IBM Watson Lab?

A Yes.

Q Was there anyone there from outside IBM?

A I don't know.

Q Was it advertised outside IBM?

A I don't know. I suspect not.

Q How long was the talk?

A I don't remember clearly. My best of my belief, it must have been around an hour. Typical afternoon seminar talk.

Q And could you briefly summarize the subject matter of the talk?

A Could I briefly summarize the subject matter of the talk?

Q Just in a couple sentences.

A Well, frankly, no. I have not looked at these slides. And beyond the title, which suggests that its contents probably survey the contents of the paper by the same title, I couldn't, no.

Q Okay. How about the page that's about ten pages in?

MR. FLINN: It should have a Bates number.

THE WITNESS: But he didn't have one.

MR. SCHLAFLY: Titled "Discrete Exponential."

MR. FLINN: DIF 055?

THE WITNESS: Right.

MR. MOORE: 55?

MR. FLINN: And your question is...?

Q BY MR. SCHLAFLY: Do you remember what you talked about in relation to this slide?

A Beyond what the slide says, no.

Q Do you recall whether or not you discussed exponential key exchange?

A I expect I did.

Q How about the page about another ten pages later entitled "Discrete Exponential Scheme"?

MR. FLINN: Page DIF 063?

THE WITNESS: I'm looking at it.

Q BY MR. SCHLAFLY: Do you recall what

you discussed in relation to that slide?

A No. Beyond -- beyond what the slide says, I -- I don't recall the giving of the lecture. I recall being in the room, but at twenty years nearly removed --

Q Was it exponential key exchange?

MR. FLINN: Was what exponential key exchange? "It" is undefined.

MR. SCHLAFLY: The discussion related to this slide.

MR. FLINN: Objection. Asked and answered. He tells you he doesn't remember what was discussed about the slide.

THE WITNESS: I believe the phrase discrete exponential scheme is synonymous on this slide with exponential key exchange.

Q BY MR. SCHLAFLY: Okay. Was this talk -- was there an understanding of confidentiality at this talk?

A I don't know. I don't remember imposing any such condition. I don't know what IBM's policies are.

Q Were any of these slides marked confidential?

A I haven't looked at them in twenty years. I'm sure they aren't.

Q Do you recall placing any restrictions on the audience on who they can talk with regarding this subject matter?

A I do not.

Q Do you recall any conversations with particular members of the audience?

MR. FLINN: At the time of the lecture?

MR. SCHLAFLY: At the time of the lecture, yes. That is before, after, during.

THE WITNESS: I remember talking to Rabin. I'm sorry, I can't think of his first name at this instant. Michael, I believe.

Q BY MR. SCHLAFLY: Michael Rabin?

A And I recall talking to the head of the mathematics department after the lecture. I don't remember who he was. And I recall that he clearly had not understood the lecture.

Q Did anyone ask questions that indicated they did understand the lecture?

A I think Michael Rabin understood the lecture.

Q And this is the Michael Rabin who is a well-known cryptographer?

A He's a well-known I would have said mathematician.

Q Well, okay. Whatever. I don't know what he is. There's some variant of RSA that's due to him, I think?

A Yes.

Q And he has maybe some kind of primality test? I'm just going on my memory. That's the same Michael Rabin?

A The same Michael Rabin.

Q And he worked for IBM at the time?

A I believe he had some split arrangement where he spent some time at IBM and some time at other places. Perhaps some were at MIT and some were in Israel.

Q Did you hand out any papers at the talk?

A I don't believe so.

Q Did you tell the audience of the existence of the "New Directions" IEEE paper?

A I don't remember.

Q Did you indicate --

A It's hard to believe I didn't.

Q Well, I do notice the title of this lecture is the same as the IEEE paper.

A Is identical. So it seems very likely if you like this kind of thing, you can read more about it in November or something like that. I'm sure I didn't know the publication date yet, but --

Q Did you make pre-prints available in any way?

A I don't remember doing so.

Q Did you in any way announce the availability of pre-prints from Stanford or Hellman or anyone else?

A Don't know.

Q Do you know if anyone there obtained a pre-print?

A I don't know:

Q Do you know if anyone obtained a pre-print to the "New Directions" IEEE paper prior to September of 1976?

A No, I don't know that, either.

Q It's not in your recollection?

A That's right.

MR. FLINN: That's been asked and answered.

Q BY MR. SCHLAFLY: Is it possible that it happened and you forgot?

MR. FLINN: Objection. Calls for speculation. You don't have to answer that. Ask another question.

Q BY MR. SCHLAFLY: Okay. Turn to Exhibit V.

A I have it in hand.

Q Page 563.

A I've got it.

Q Do you see the section entitled Roman numeral III, "Trap-Door Knapsacks"?

A Uh-huh.

Q Do you see the paragraph right above it?

11

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DEPARTMENT 4

BEFORE THE HONORABLE SPENCER WILLIAMS, JUDGE

ROGER SCHLAFLY,

PLAINTIFF,

-vs-

PUBLIC KEY PARTNERS,

DEFENDANT,

Consolidated C-94-20512-SW
and C-96-20094-SW
CONFIDENTIAL PROCEEDINGS

---oOo---

REPORTER'S TRANSCRIPT OF PROCEEDINGS

THURSDAY, FEBRUARY 29, 1996

APPEARANCES:

FOR RSA:	HELLER, EHRMAN, WHITE & MCAULIFFE BY: ROBERT T. HASLAM, ESQUIRE -AND- ROBERT D. FRAM, ESQUIRE -AND- CAROLYN R. BOSTICK
FOR CARO-KANN:	ALSTON & BIRD PATRICK J. FLINN, ESQUIRE MORRISON & FOERSTER BY: KARL J. KRAMER, ESQUIRE -AND- JANA G. GOLD, ESQUIRE
FOR DR. ROGER SCHLAFLY:	IN PROPER PERSON
FOR PKP:	THOMAS HOGAN, ESQUIRE
COURT REPORTER:	BRYNN DOCKSTADER, CSR, CMR CERTIFICATE NO. 3518

in this case that there was an open sale bar. And in giving that, what is the significance of the three other publications of the conferences? The National Computer, the EEE information theory and the presentation privately to IBM?

The significance of that to you is they had no incentive. Every indication in this record is that tl wanted to get this thing out in the public domain as quickly and as broadly as possible.

The Howmedica case and the Tyler case do indicate given the breadth of the disclosure of those three conferences with the slides, that is, that alone might.

I recognize here it is an extension of district court cases. That alone in the context of this case might satisfy the printed publication because it is undisputed on this record that those slides and those presentations taught every one of interest and the interested public how to practice these patents. We don't have to stop here. And we know what happened after that.

And I want to touch on the MIT case because I think we can meet the MIT criteria right now. In the MIT case there was one presentation of 50 to 500 people with one article presented to the head of the conference prior to the conference and six copies disseminated after the breeches of fiduciary duty and whether or not there was a license, whether to dissolve a partnership.

If they dissolve the partnership who gets what? They were concerned that the breadth taken out of context as is now being done might work to CKC's detriment.

With respect to the Vaeck case and the cases on the scope of enablement necessarily related to the breadth of the claims that are not in the 12 paragraphs, two cases. Those are not dealing with whether the claim is definite, and one can understand it. Those are cases which say it doesn't matter whether the claim is definite and you understand it. You can't pre-empt the future by such a broad claim unless you tell people how to find the breadth to that claim.

On the 870 and the public printed publication, the record will say what it says. I do not contend that the law says that mere oral presentations are alone sufficient.

I do say, however, that the Howmedica case and I believe it is Tyler, both district court cases, both stand for the proposition in this case. And I think it is an extension of the law. But I think it is grounded on the principles underlying 102B. Those presentations with the printed slide do constitute a publication.

On accessibility, the test is accessibility to